Project Introduction

Validating software is a critical step in developing high confidence systems. Typical software development practices are not acceptable in systems where failure leads to loss of life or other high costs. New software development tools are needed to radically reduce defect rates and enable the high levels of confidence required for safety- and security-critical systems. Lightweight verification techniques have proven themselves effective in finding defects in large software systems by balancing rigor with scalability and usability. Lightweight verification techniques do not exhaustively check software, but they can find defects in systems that are too large for more rigorous analysis techniques, and are fast becoming an essential tool for software developers. The techniques generally fail to address key sources of problems specific to embedded systems: paths due to asynchronous transfer of control or context switches between tasks are not considered; assembly language components are ignored; it is hard to detect violations of domain-specific rules. We propose to extend and adapt our static analysis technology to make it capable of addressing these problems. We will exploit our existing connections with NASA facilities to gain help validating our approach and to ensure that the solution we propose is responsive to NASA's unique needs.

Anticipated Benefits

Potential NASA Commercial Applications: Lightweight verification tools such as CodeSonar are becoming increasingly popular in many industrial sectors, especially those concerned with developing high-confidence real-time embedded software. This includes communications, military/aerospace, medical devices, automotive, finance, security, and others. If successful, the technology we propose to develop will provide the capability to find more serious flaws in such software than current approaches, thereby cutting development costs and increasing code quality.

Static Detection of Bugs in Embedded Software using Lightweight Verification, Phase I

Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Center / Facility:
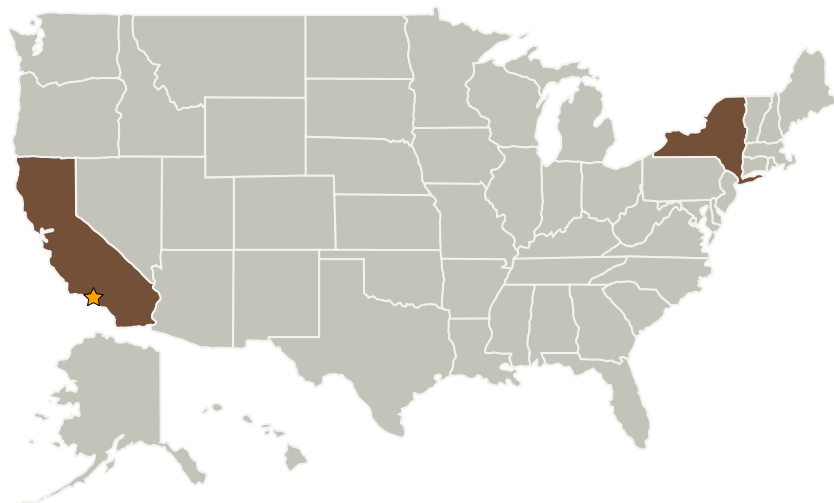
Jet Propulsion Laboratory (JPL)

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Primary U.S. Work Locations and Key Partners

Organizations Performing Work	Role	Type	Location
⭐Jet Propulsion Laboratory(JPL)	Lead Organization	NASA Center	Pasadena, California
GrammaTech, Inc.	Supporting Organization	Industry	Ithaca, New York

Primary U.S. Work Locations	
California	New York

Project Transitions

▶ **January 2007:** Project Start

✔ **July 2007:** Closed out

   Closeout Summary: Static Detection of Bugs in Embedded Software using Lightweight Verification, Phase I Project Image

Project Management

Program Director:
Jason L Kessler

Program Manager:
Carlos Torrez

Project Manager:
Celestino Jun Rosca

Principal Investigator:
Ray Teitelbaum

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  └ TX11.1 Software Development, Engineering, and Integrity
    └ TX11.1.2 Verification and Validation of Software systems